



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/033,373

10/29/2001

Eduard K. de Jong

SUN-P7014

7801

24209

7590

10/20/2006

GUNNISON MCKAY & HODGSON, LLP  
1900 GARDEN ROAD  
SUITE 220  
MONTEREY, CA 93940

EXAMINER

NGUYEN, THU HA T

ART UNIT

PAPER NUMBER

2155

DATE MAILED: 10/20/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

10/033,373

Applicant(s)

DE JONG ET AL.

Examiner

Thu Ha T. Nguyen

Art Unit

2155

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 04 August 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-6 and 8 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-6 and 8 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date 7/28/06.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_.

### **DETAILED ACTION**

1. Claims **1-6, and 8** are presented for examination.
2. Claims 1-6 and 8 are currently amended.

### **Response to Arguments**

3. Applicant's arguments filed August 04, 2006 have been fully considered but they are not persuasive because of the following reasons:

4. Applicant argues that Win does not teach or suggest said service provider capable of communicating directly with said authority to dynamically authenticate said enrollment results wherein said service provider is an entity that is different from an entity that is said authority.

In response to applicant argument, the examiner submits that Win teaches a runtime module 206 (figure 2) on the protected server 104 (i.e., service provider) (figure 2) receives the user request, including cookie in the request, to use the resource. The runtime module 206 connects to an access server 106 (i.e., authority) (figure 2) that can determine whether a particular user is authentic and which resources the user is authorized to access by using cookie to authenticate (see abstract). Therefore, Win does teach the step of the server service provider capable of communicating directly with said authority to dynamically authenticate said enrollment results upon receives that HTTP/URL request, and the protected server 104 is different with the access server 106.

Art Unit: 2155

5. As a result, cited prior art does disclose a system and method for obtaining service on a data communications network, as broadly claimed by the Applicants. Applicants clearly have still failed to identify specific claim limitations that would define a clearly patentable distinction over prior art.

Therefore, the examiner asserts that cited prior art teaches or suggests the subject matter broadly recited in independent claims 1-6, and 8. Accordingly, claims 1-6, and 8 are also rejected at least by the reasons set forth in this office action below.

### **Claim Rejections - 35 USC § 102**

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless --

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-6, 8 and 10 are rejected under 35 U.S.C. §102(e) as being anticipated by **Win et al.** (hereinafter Win) U.S. Patent No. **6,453,353**.

8. As to claim 1, **Win** teaches the invention as claimed, including a method for obtaining a service on a data communications network, the method comprising:  
enrolling with an authority, said enrolling creating enrollment results, said enrollment results comprising user data in a credential used for user authentication

Art Unit: 2155

(abstract, figures 1, 5, col. 6, lines 19-54, col. 9, lines 14-col. 11, lines 9, col. 22, lines 47-64 –*enrolling/registering user information and user's role with registry server 108 and access server 106 (i.e., authority), the access server 106 authorizes user, creates user cookies and roles cookies (i.e., enrollment results) and sends to browser 100 (i.e., user); and*

using said enrollment results to obtain a service from a service provider (figure 1, protected server 104) on said data communications network (abstract, figures 1, 3B-C, col. 6, lines 58-65, col. 7, line 15-col. 8, line 63, col. 22, line 47-col. 23, line 9 –*user using/browser 100 passing returned results (i.e., user cookies and roles cookies) to access protected server 104 (i.e., service provider) for requesting to use the resource),* said service provider capable of communicating with said authority to dynamically authenticate said enrollment results (*a runtime module 206 (figure 2) on the protected server 104 (i.e., service provider) (figure 2) receives the user request, including cookie in the request, to use the resource. The runtime module 206 connects to an access server 106 (i.e., authority) (figure 2) that can determine whether a particular user is authentic and which resources the user is authorized to access (see abstract))* wherein said service provider (figure 1, protected server 104) is an entity that is different from an entity that is said authority (figure 1, access server 106) (figures 1, protected server 104, figure 1 (i.e., service provider) is separated and different from access server 106, figure 1 (i.e., authority)).

Art Unit: 2155

9. As to claim 2, **Win** teaches the invention as claimed, including a method for managing identification in a data communications network, the method comprising:

generating a credential including authenticated user data (figures 5A-C, col. 10, lines 41-63 – *creates user cookies and roles cookies (i.e., enrollment results) and sends to browser 100 (i.e., user)*), said generating comprising:

presenting a request for authenticated user data and a first set of user data to an authority (figures 5A-C, col. 9, lines 14-67 –*sending request including user information and user role to registry server 108 and access server 106 (i.e., authority)*); and

receiving said credential including said authenticated user data from said authority in response to said request (figures 5A-C, col. 9, line 51-col. 10, line 63 –*the access server 106 (i.e., authority) after authenticate user information and returns result (i.e., user cookies and roles cookies) to browser 100*); and

using said credential including said authenticated user data to obtain at least one service on said data communications network (figures 3B-C, col. 6, lines 41-65, col. 7, line 15-col. 8, line 63, col. 22, line 47-col. 23, line 9 –*user using/browser 100 passing returned results (i.e., user cookies and roles cookies) to access protected server 104 (i.e., service provider) for requesting to use the resource*), said using comprising:

presenting a service request and said credential including said authenticated user data to a service provider on said data communications network (figures 3B-C, col. 6, lines 41-65, col. 7, line 15-col. 8, line 63, col. 22, line 47-col. 23, line 9 –*issuing HTTP request/URL including cookie to protected server 104 (figure 1)*); and

receiving said at least one service in response to said service request if said service provider determines said authenticated user data is sufficient to provide said at least one service (abstract, figures1, 3B-C, col. 6, lines 17-54, col. 8, lines 5-col. 9, lines 12, col. 22, line 47-col. 23, line 9 –*the protected server 104 determines whether the HTTP request/URL request, including user cookie, is a protected resource and the user cookie is authenticated and the user is authenticated then returns resource pages to browser 100*) wherein said service provider is capable of communicating with said authority to dynamically authenticate said authenticated user data (*a runtime module 206 (figure 2) on the protected server 104 (i.e., service provider) (figure 2) receives the user request, including cookie in the request, to use the resource. The runtime module 206 connects to an access server 106 (i.e., authority) (figure 2) that can determine whether a particular user is authentic and which resources the user is authorized to access (see abstract))*) and further wherein said service provider is an entity that is different from an entity that is said authority (figures1, *protected server 104, figure 1 (i.e., service provider) is separated and different from access server 106, figure 1 (i.e., authority)*)).

10. As to claim 3, **Win** teaches the invention as claimed, including a program storage device readable by a machine, embodying a program of instructions executable by the machine to perform a method for obtaining a service on a data communications network, the method comprising:

enrolling with an authority, said enrolling creating enrollment results, said enrollment results comprising user data in a credential used for user authentication (abstract, figures 1, 5, col. 6, lines 19-54, col. 9, lines 14-col. 11, lines 9, col. 22, lines 47-64 –*enrolling/registering user information and user's role with registry server 108 and access server 106 (i.e., authority), the access server 106 authorizes user, creates user cookies and roles cookies (i.e., enrollment results) and sends to browser 100 (i.e., user); and*

using said enrollment results to obtain a service from a service provider on said data communications network (abstract, figures 1, 3B-C, col. 6, lines 17-54, col. 8, lines 5-col. 9, lines 12, col. 22, line 47-col. 23, line 9 –*the protected server 104 determines whether the HTTP request/URL request, including user cookie, is a protected resource and the user cookie is authenticated and the user is authenticated then returns resource pages to browser 100*), said service provider capable of communicating with said authority to dynamically authenticate said enrollment results (*a runtime module 206 (figure 2) on the protected server 104 (i.e., service provider) (figure 2) receives the user request, including cookie in the request, to use the resource. The runtime module 206 connects to an access server 106 (i.e., authority) (figure 2) that can determine whether a particular user is authentic and which resources the user is authorized to access (see abstract)) wherein said service provider is an entity that is different from an entity that is said authority (figures 1, protected server 104, figure 1 (i.e., service provider) is separated and different from access server 106, figure 1 (i.e., authority)).*



Art Unit: 2155

11. As to claim 4, **Win** teaches the invention as claimed, including a program storage device readable by a machine, embodying a program of instructions executable by the machine to perform a method for managing identification in a data communications network, the method comprising:

generating a credential including authenticated user data (figures 5A-C, col. 10, lines 41-63 – *creates user cookies and roles cookies (i.e., enrollment results) and sends to browser 100 (i.e., user)*), said generating comprising:

presenting a request for authenticated user data and a first set of user data to an authority (figures 5A-C, col. 9, lines 14-67 –*sending request including user information and user role to registry server 108 and access server 106 (i.e., authority)*); and

receiving said credential including said authenticated user data from said authority in response to said request (figures 5A-C, col. 9, line 51-col. 10, line 63 –*the access server 106 (i.e., authority) after authenticate user information and returns result (i.e., user cookies and roles cookies) to browser 100*); and

using said credential including said authenticated user data to obtain at least one service on said data communications network (figures 3B-C, col. 6, lines 41-65, col. 7, line 15-col. 8, line 63, col. 22, line 47-col. 23, line 9 –*user using/browser 100 passing returned results (i.e., user cookies and roles cookies) to access protected server 104 (i.e., service provider) for requesting to use the resource*), said using comprising:

presenting a service request and said credential including said authenticated user data to a service provider on said data communications network (figures 3B-C, col.

Art Unit: 2155

6, lines 41-65, col. 7, line 15-col. 8, line 63, col. 22, line 47-col. 23, line 9 –*issuing HTTP request/URL including cookie to protected server 104 (figure 1)*); and

receiving said at least one service in response to said service request if said service provider determines said authenticated user data is sufficient to provide said at least one service (abstract, figures1, 3B-C, col. 6, lines 17-54, col. 8, lines 5-col. 9, lines 12, col. 22, line 47-col. 23, line 9 –*the protected server 104 determines whether the HTTP request/URL request, including user cookie, is a protected resource and the user cookie is authenticated and the user is authenticated then returns resource pages to browser 100*) wherein said service provider is capable of communicating with said authority to dynamically authenticate said authenticated user data (*a runtime module 206 (figure 2) on the protected server 104 (i.e., service provider) (figure 2) receives the user request, including cookie in the request, to use the resource. The runtime module 206 connects to an access server 106 (i.e., authority) (figure 2) that can determine whether a particular user is authentic and which resources the user is authorized to access (see abstract)*) and further wherein said service provider is an entity that is different from an entity that is said authority (figures1, *protected server 104, figure 1 (i.e., service provider) is separated and different from access server 106, figure 1 (i.e., authority)*)).

12. As to claim 5, **Win** teaches the invention as claimed, including an apparatus for managing identification in a data communications network, the apparatus comprising:

Art Unit: 2155

means for generating a credential including said authenticated user data (figures 5A-C, col. 10, lines 41-63 – *creates user cookies and roles cookies (i.e., enrollment results) and sends to browser 100 (i.e., user)*), said means of generating comprising:

means for presenting a request for authenticated user data and a first set of user data to an authority (figures 5A-C, col. 9, lines 14-67 –*sending request including user information and user role to registry server 108 and access server 106 (i.e., authority)*); and

means for receiving said credential including said authenticated user data from said authority in response to said request (figures 5A-C, col. 9, line 51-col. 10, line 63 – *the access server 106 (i.e., authority) after authenticate user information and returns result (i.e., user cookies and roles cookies) to browser 100*); and

means for using said credential including said authenticated user data to obtain at least one service on said data communications network (figures 3B-C, col. 6, lines 41-65, col. 7, line 15-col. 8, line 63, col. 22, line 47-col. 23, line 9 –*user using/browser 100 passing returned results (i.e., user cookies and roles cookies) to access protected server 104 (i.e., service provider) for requesting to use the resource*), said means for using comprising:

means for presenting a service request and said credential including said authenticated user data to a service provider on said data communications network (figures 3B-C, col. 6, lines 41-65, col. 7, line 15-col. 8, line 63, col. 22, line 47-col. 23, line 9 –*issuing HTTP request/URL including cookie to protected server 104 (figure 1)*); and

means for receiving said at least one service in response to said service request if said service provider determines said authenticated user data is sufficient to provide said at least one service (abstract, figures1, 3B-C, col. 6, lines 17-54, col. 8, lines 5-col. 9, lines 12, col. 22, line 47-col. 23, line 9 –*the protected server 104 determines whether the HTTP request/URL request, including user cookie, is a protected resource and the user cookie is authenticated and the user is authenticated then returns resource pages to browser 100*) wherein said service provider is capable of communicating with said authority to dynamically authenticate said authenticated user data (*a runtime module 206 (figure 2) on the protected server 104 (i.e., service provider) (figure 2) receives the user request, including cookie in the request, to use the resource. The runtime module 206 connects to an access server 106 (i.e., authority) (figure 2) that can determine whether a particular user is authentic and which resources the user is authorized to access (see abstract)*) and further wherein said service provider is an entity that is different from an entity that is said authority (*a figures1, protected server 104, figure 1 (i.e., service provider) is separated and different from access server 106, figure 1 (i.e., authority)*)).

13. As to claim 6, **Win** teaches the invention as claimed, including an apparatus for managing identification in a data communications network, the apparatus comprising:

means for receiving a user-controlled secure storage device (figures 1, 5A-C, col. 9, lines 51-col. 10, lines 26, i.e., registry repository 110);

Art Unit: 2155

means for enrolling said user with an authority, said enrolling comprising providing information requested by said authority (abstract, figures 1, 5, col. 6, lines 19-54, col. 9, lines 14-col. 11, lines 9, col. 22, lines 47-64 –*enrolling/registering user information and user's role with registry server 108 and access server 106 (i.e., authority), the access server 106 authorizes user, creates user cookies and roles cookies (i.e., enrollment results) and sends to browser 100 (i.e., user);*

means for receiving a credential including user data, in response to said enrolling, wherein said credential is used for user authentication (figures 5A-C, col. 9, line 51-col. 10, line 63 –*the access server 106 (i.e., authority) after authenticate user information and returns result (i.e., user cookies and roles cookies) to browser 100);*

means for storing said credential including said user data in said user-controlled secure storage device (figures 5A-C, col. 6, lines 20-65, col. 9, lines 33-col. 10, line 55 –*storing users information users roles in registry server 108 and registry repository 110);* and

means for using said credential including said user data at a service provider Web site to obtain a service wherein said service provider web site is capable of communicating with said authority to dynamically authenticate said authenticated user data (a runtime module 206 (figure 2) on the protected server 104 (i.e., service provider) (figure 2) receives the user request, including cookie in the request, to use the resource. The runtime module 206 connects to an access server 106 (i.e., authority) (figure 2) that can determine whether a particular user is authentic and which resources the user is authorized to access (see abstract)) and further wherein said service provider Web site

Art Unit: 2155

is an entity that is different from an entity that is said authority (figures1, *protected server 104, figure 1 (i.e., service provider) is separated and different from access server 106, figure 1 (i.e., authority)*)).

14. As to claim 8, **Win** teaches the invention as claimed, including an apparatus for obtaining a service on a data communications network, the apparatus comprising:

a service provider configured to accept a service request and a credential including enrollment results obtained from an enrollment authority (figures 3B-C, col. 6, lines 41-65, col. 7, line 15-col. 8, line 63, col. 22, line 47-col. 23, line 9 –*issuing HTTP request/URL including cookie, that is obtain from access server 106, to protected server 104 (figure 1)*), said service provider capable of communicating with said authority to dynamically authenticate said enrollment results (*a runtime module 206 (figure 2) on the protected server 104 (i.e., service provider) (figure 2) receives the user request, including cookie in the request, to use the resource. The runtime module 206 connects to an access server 106 (i.e., authority) (figure 2) that can determine whether a particular user is authentic and which resources the user is authorized to access (see abstract)*), said service provider configured to provide said service based upon said enrollment results and a response from said enrollment authority (abstract, figures1, 3B-C, col. 6, lines 17-54, col. 8, lines 5-col. 9, lines 12, col. 22, line 47-col. 23, line 9 –*the protected server 104 determines whether the HTTP request/URL request, including user cookie, is a protected resource and the user cookie is authenticated and the user is*

Art Unit: 2155

*authenticated then returns resource pages to browser 100), wherein said service provider is an entity that is different from an entity that is said authority (figures1, protected server 104, figure 1 (i.e., service provider) is separated and different from access server 106, figure 1 (i.e., authority)).*

15. As to claim 10, **Win** teaches the invention as claimed, including an apparatus for managing identification in a data communications network, the apparatus comprising: a service provider configured to accept a service request (figures 3B-C, col. 6, lines 57-65, col. 8, lines 1-63 –*protected server 104 (i.e., service provider) receives user HTTP/URL request*), a credential including a first set of user data and a second set of user data including support information for said credential, said first set of user data comprising user data authenticated by an authority (figures 3B-C, col. 6, lines 17-65, col. 8, lines 5-col. 9, lines 12, col. 22, line 47-col. 23, line 9 –*access server authenticates user information and creates/generates user cookie and roles cookies*), said service provider further configured to determine whether said first set of user data and said second set of user data are sufficient to provide said service, said service provider further configured to provide said service based upon said determination (abstract, figures1, 3B-C, col. 6, lines 17-54, col. 8, lines 5-col. 9, lines 12, col. 22, line 47-col. 23, line 9 –*the protected server 104 determines whether the HTTP request/URL request, including user cookie, is a protected resource and the user cookie is authenticated and the user is authenticated then returns resource pages to browser 100*), wherein said service provider is an entity that is different from an entity that is said

*authority (figures 1, protected server 104, figure 1 (i.e., service provider) is separated and different from access server 106, figure 1 (i.e., authority)).*

### **Conclusion**

16. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thu Ha Nguyen, whose telephone number is (571) 272-3989. The examiner can normally be reached Monday through Friday from 8:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Najjar Saleh, can be reached at (571) 272-4006.

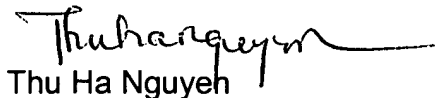
The fax phone numbers for the organization where this application or proceeding



Art Unit: 2155

is assigned are (571) 273-8300 for regular communications.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Thu Ha Nguyeh

October 12, 2006